FORTINET
High Performance Network Security

FortiOS™ Handbook - Managing Devices

VERSION 5.4.0

FORTIOS
5.4
VERSION

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Monday, December 21, 2015

FortiOS™ Handbook - Managing Devices

01-540-122871-20151221

TABLE OF CONTENTS

Change Log

Date	Change Description
	New FortiOS 5.4 Release
2015-02-18	Branched document from FortiOS 5.2 document.
2015-10-27	Removed Vulnerability Scan feature, which is now provided by FortiClient.

Introduction

Welcome and thank you for selecting Fortinet products for your network protection.

This chapter contains the following topics:

Before you begin

Before you begin using this guide, please ensure that:

- You have administrative access to the web-based manager and/or CLI.
- The FortiGate unit is integrated into your network.
- The operation mode has been configured.
- The system time, DNS settings, administrator password, and network interfaces have been configured.
- Firmware, FortiGuard Antivirus and FortiGuard Antispam updates are completed.
- Any third-party software or servers have been configured using their documentation.

While using the instructions in this guide, note that administrators are assumed to be super_admin administrators unless otherwise specified. Some restrictions will apply to other administrators.

How this guide is organized

This handbook chapter contains the following sections:

Managing “bring your own device” describes device monitoring, devices, device groups, and device policies. The administrator can monitor all types of devices and control their access to network resources.

What's New in FortiOS 5.4

802.1x Mac Authentication Bypass (197218)

Some FortiGate models contain a hardware switch. On the hardware switch interface, 802.1X authentication is available. You might want to bypass 802.1X authentication for devices such as printers that cannot authenticate, identifying them by their MAC address.

In the CLI, enable MAC authentication bypass on the interface:

```
config system interface
   edit "lan"
      set ip 10.0.0.200 255.255.255.0
      set security-mode 802.1X
      set security-mac-auth-bypass enable
      set security-groups "Radius-group"
   end
```

The devices that bypass authentication have entries in the RADIUS database with their MAC address in the User-Name and User-Password attributes instead of user credentials.

Vulnerability Scan status change(293156)

The FortiGate will no longer function as a vulnerability scanner, even in CLI mode. Vulnerability scans / assessments will handled by the FortiClient software.

FortiFone devices are now identified by FortiOS (289921)

FortiFone devices are now identified by FortiOS as **Fortinet FON**.

Support for MAC Authentication Bypass (MAB) (197218)

MAC Authentication Bypass allows devices without 802.1X capability (printers and IP phones for example) to bypass authentication and be allowed network access based on their MAC address. This feature requires RADIUS-based 802.1X authentication in which the RADIUS server contains a database of authorized MAC addresses.

MAC Authentication Bypass is configurable only in the CLI and only on interfaces configured for 802.1X authentication. For example:

```
config system interface
   edit "lan"
      set ip 10.0.0.200 255.255.255.0
      set vlanforward enable
      set security-mode 802.1X
      set security-mac-auth-bypass enable
      set security-groups "Radius-group"
   end
end
```

MAC Authentication Bypass is also available on WiFi SSIDs, regardless of authentication type. It is configurable only in the CLI. You need to enable the `radius-mac-auth` feature and specify the RADIUS server that will be used. For example:

```
config wireless-controller vap
   edit "office-ssid"
      set security wpa2-only-enterprise
      set auth usergroup
      set usergroup "staff"
      set radius-mac-auth enable
      set radius-mac-auth-server "ourRadius"
   end
end
```

Active device identification (279278)

Hosts whose device type cannot be determined passively are actively scanned using the same techniques as the vulnerability scan. This active scanning is enabled by default on models that support vulnerability scanning. You can turn off Active Scanning on any interface. In the GUI, go to the interface's page in **Network > Interfaces**.

CLI Syntax:

```
config system interface
   edit port1
      set device-identification enable
      set device-identification-active-scan disable
   end
```

Device Page Improvements (Detected and custom devices) (280271)

Devices are now in two lists on the **User & Device** menu. Detected devices are listed in the **Device List** where you can list them alphabetically, by type, or by interface. On the **Custom Devices and Groups** page you can

- create custom device groups
- predefine a device, assigning its device type and adding it to custom device groups

Device offline timeout is adjustable (269104)

A device is considered offline if it has not sent any packets during the timeout period. Prior to FortiOS 5.4, the timeout value was fixed at 90 seconds. Now the timeout can be set to any value from 30 to 31 536 000 seconds (365 days). The default value is 300 seconds (5 minutes). The timer is in the CLI:

```
config system global
   set device-idle-timeout 300
end
```

Improved detection of FortiOS-VM devices (272929)

A FortiGate-VM device is an instance of FortiOS running on a virtual machine (VM). The host computer does not have the Fortinet MAC addresses usually used to detect FortiGate units. Device detection now has two additional ways to detect FortiGate-VMs:

- the FortiGate vendor ID in FortiOS IKE messages
- the FortiGate device ID in FortiGuard web filter and spamfilter requests

Custom avatars for custom devices (299795)

You can upload an avatar for a custom device. The avatar is then displayed in the GUI wherever the device is listed, such as FortiView, log viewer, or policy configuration. To upload an avatar image,click Upload Image on the New Device or Edit Device page of **User & Device > Custom Devices & Groups**. The image can be in any format your browser supports and will be automatically sized to 36 x 36 pixels for use in the FortiGate GUI.

Managing “bring your own device”

FortiOS can control network access for different types of personal mobile devices that your employees bring onto your premises. You can:

- identify and monitor the types of devices connecting to your networks, wireless or wired
- use MAC address based access control to allow or deny individual devices
- create security policies that specify device types
- enforce endpoint control on devices that can run FortiClient Endpoint Control software

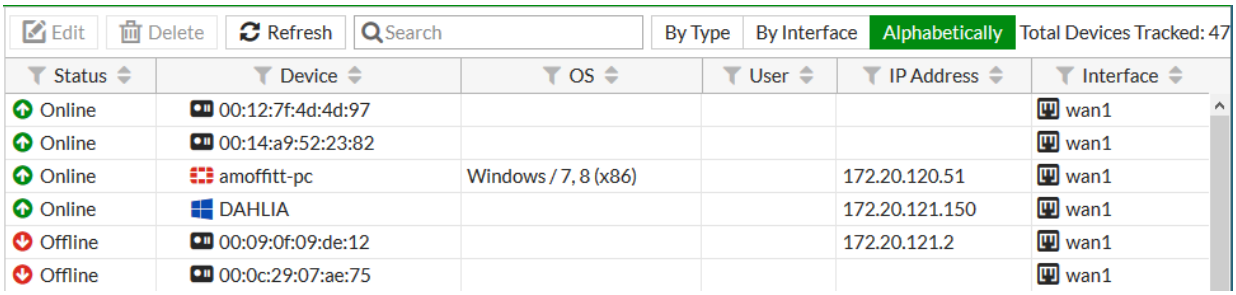
This chapter contains the following sections:

Device monitoring

The FortiGate unit can monitor your networks and gather information about the devices operating on those networks. Collected information includes:

- MAC address
- IP address
- operating system
- hostname
- user name
- how long ago the device was detected and on which FortiGate interface

You can go to **User & Device > Device List** to view this information. Mouse-over the **Device** column for more details.



Depending on the information available, the Device column lists the Alias or the MAC address of the device. For ease in identifying devices, Fortinet recommends that you assign each device an Alias.

Device monitoring is enabled separately on each interface. Device detection is intended for devices directly connected to your LAN ports. If enabled on a WAN port, device detection may be unable to determine the

operating system on some devices. Hosts whose device type cannot be determined passively can be found by enabling active scanning on the interface.

You can also manually add devices. This enables you to ensure that a device with multiple interfaces is displayed as a single device.

To configure device monitoring

1. Go to **Network > Interfaces**.
2. Edit the interface that you want to monitor devices on.
3. In **Networked Devices**, turn on **Device Detection** and optionally turn on **Active Scanning**.
4. Select **OK**.
5. Repeat steps 2 through 4 for each interface that will monitor devices.

To assign an alias to a detected device or change device information

1. Go to **User & Device > Device List** and edit the device entry.
2. Enter an **Alias** such as the user’s name to identify the device.
3. Change other information as needed.
4. Select **OK**.

To add a device manually

1. Go to **User & Device > Custom Devices & Groups**.
2. Select **Create New > Device**.
3. Enter the following information:
   - Alias (required)
   - MAC address
   - Additional MACs (other interfaces of this device)
   - Device Type
   - Optionally, add the device to **Custom Groups**.
   - Optionally, enter **Comments**.
3. Select **OK**.

Device Groups

You can specify multiple device types in a security policy. As an alternative, you can add multiple device types to a custom device group and include the group in the policy. This enables you to create a different policy for devices that you know than for devices in general.

To create a custom device group and add devices to it

1. Go to **User & Device > Custom Devices & Groups**.
   The list of device groups is displayed.
2. Select **Create New > Device Group**.
3. Enter a **Name** for the new device group.

4. Click in the **Members** field and click a device type to add. Repeat to add other devices.
5. Select **OK**.

Controlling access with a MAC Address Access Control List

A MAC Address Access Control List (ACL) allows or blocks access on a network interface that includes a DHCP server. If the interface does not use DHCP, or if you want to limit network access to a larger group such as employee devices, it is better to create a device group and specify that group in your security policies.

A MAC Address ACL functions as either

- a list of devices to block, allowing all other devices

or

- a list of devices to allow, blocking all other devices

Allowed devices are assigned an IP address. The Assign IP action assigns the device an IP address from the DHCP range. In a list of allowed devices, you can also use the Reserve IP action to always provide a specific IP address to the device.

The **Unknown MAC Address** entry applies to "other" unknown, unlisted devices. Its action must be opposite to that of the other entries. In an allow list, it must block. In a block list, it must allow.

To create a MAC Address ACL to allow only specific devices

1. Go to the SSID or network interface configuration.
2. In the **DHCP Server** section, expand **Advanced**.
   DHCP Server must be enabled.
3. In **MAC Reservation + Access Control**, select **Create New** and enter an allowed device’s **MAC Address**.
4. In the **IP or Action** column, select one of:
   - Assign IP — device is assigned an IP address from the DHCP server address range.
   - Reserve IP — device is assigned the IP address that you specify.
5. Repeat Steps "Controlling access with a MAC Address Access Control List" on page 13 and "Controlling access with a MAC Address Access Control List" on page 13 for each additional MAC address entry.
6. Set the **Unknown MAC Address** entry **IP or Action** to **Block**.
   Devices not in the list will be blocked.
7. Select **OK**.

To create a MAC Address ACL to block specific devices

1. Go to the SSID or network interface configuration.
2. In the **DHCP Server** section, expand **Advanced**.
   DHCP Server must be enabled.
3. In **MAC Reservation + Access Control,** select **Create New** and enter the **MAC Address** of a device that must be blocked.
4. In the **IP or Action** column, select **Block**.
5. Repeat Steps "Controlling access with a MAC Address Access Control List" on page 13 and "Controlling access with a MAC Address Access Control List" on page 13 for each device that must be blocked.

6. Set the **Unknown MAC Address** entry **IP or Action** to **Assign IP**.
   Devices not in the list will be assigned IP addresses.
7. Select **OK**.

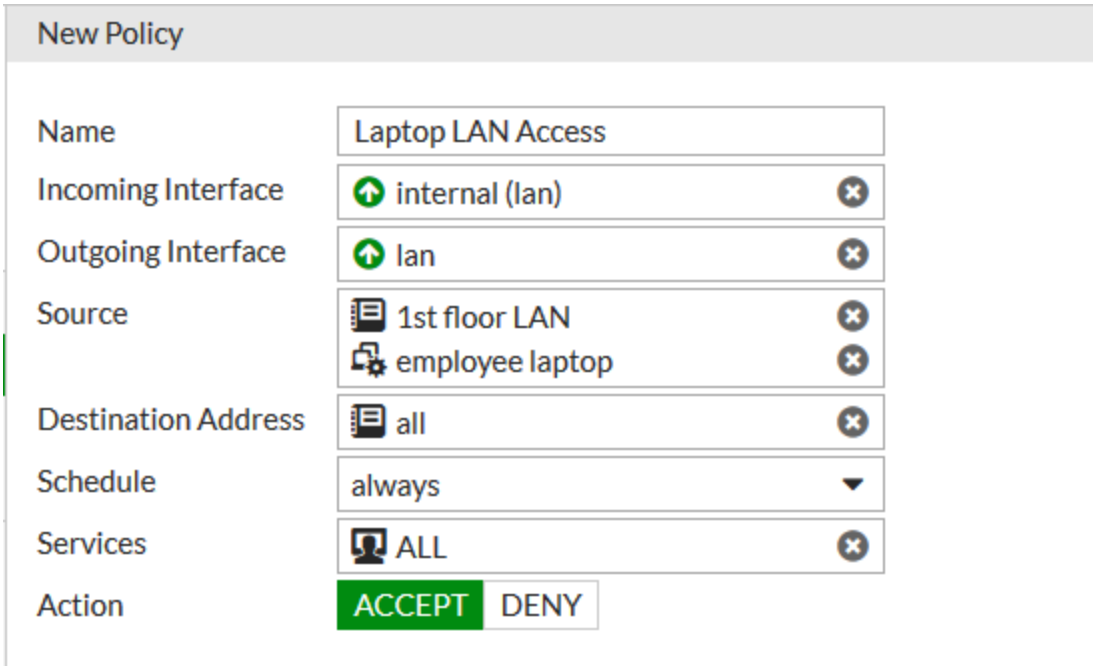
Security policies for devices

Security policies enable you to implement policies according to device type. For example:

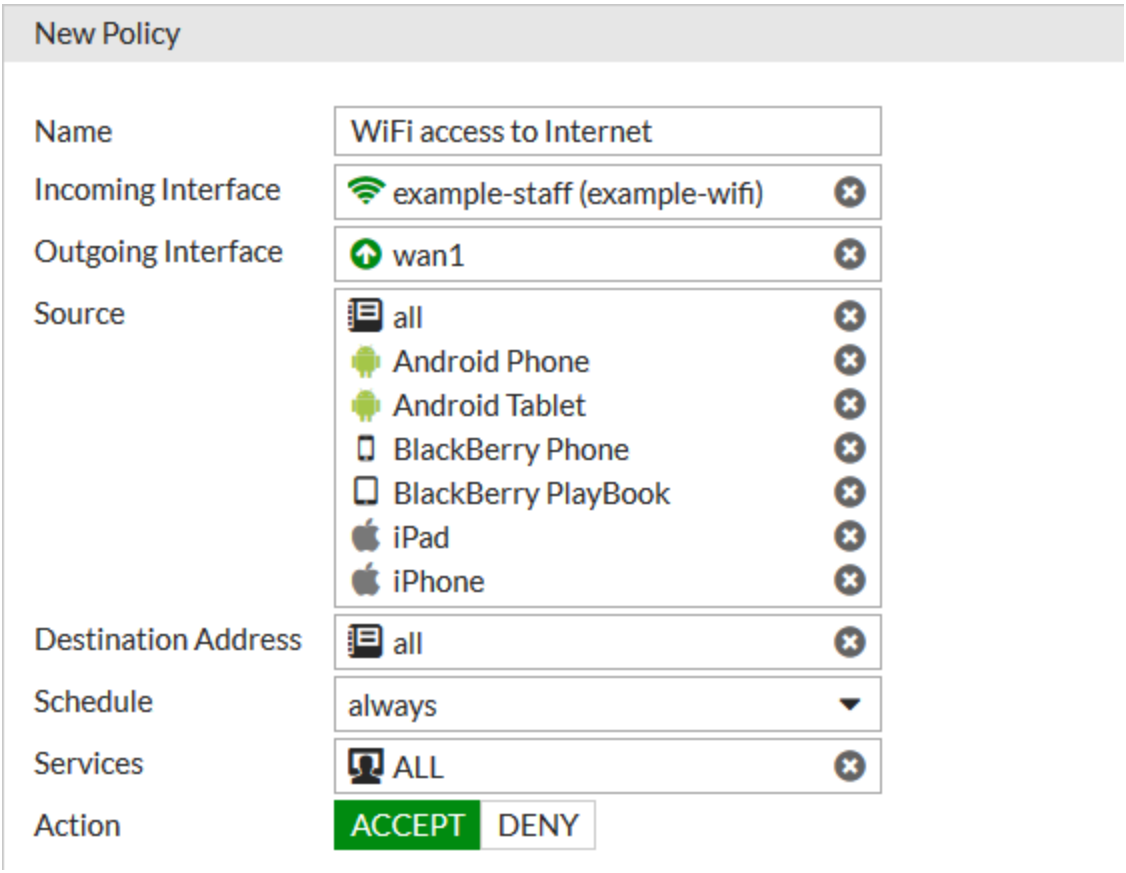
- Gaming consoles cannot connect to the company network or the Internet.
- Personal tablet and phone devices can connect to the Internet but not to company servers.
- Company-issued laptop computers can connect to the Internet and company servers. Web filtering and antivirus are applied.
- Employee laptop computers can connect to the Internet, but web filtering is applied. They can also connect to company networks, but only if FortiClient Endpoint Security is installed to protect against viruses.

The following images show these policies implemented for WiFi to the company network and to the Internet.

Device policies for company laptop access to the company network



Device policies for WiFi access to the Internet



The next section explains device policy creation in detail.

Creating device policies

Device-based security policies are similar to policies based on user identity:

- The policy enables traffic to flow from one network interface to another.
- NAT can be enabled.
- UTM protection can be applied.

To create a device policy

1. Go to **Policy & Objects > IPv4 Policy** and select **Create New**.
2. Choose **Incoming Interface**, **Outgoing Interface** and **Source** as you would for any security policy.
3. In **Source**, select an address and the device types that can use this policy.
   You can select multiple devices or device groups.
4. Turn on **NAT** if appropriate.
5. Configure **Security Profiles** as you would for any security policy.
6. Select **OK**.

Adding endpoint protection

Optionally, you can require that users’ devices connecting to a particular network interface have FortiClient Endpoint Security software installed. Devices without an up-to-date installation of FortiClient software are restricted to a captive portal from which the user can download a FortiClient installer. For information about creating FortiClient profiles, see "Endpoint Protection".

To add endpoint protection to a security policy

1. Go to **Network > Interfaces** and edit the interface.
2. In **Admission Control** turn on **Allow FortiClient Connections** and **FortiClient Enforcement**.
3. Optionally, select sources (addresses and device types) to exempt from FortiClient enforcement.
4. Optionally, select destination addresses and services to exempt from FortiClient enforcement.
5. Select **OK**.

FortiOS pushes a FortiClient profile out to the FortiClient software, configuring network protection such as antivirus, application control, and web category filtering. To create these profiles, go to **Security Profiles > FortiClient Profiles**.

FORTINET®

High Performance Network Security